Patent Application of

James T. Byers

for

TITLE: COMPUTER SYSTEM THAT PROVIDES THE DIGITIZED HUMAN FINGERPRINT AS ELECTRONIC SIGNATURE FOR DIGITAL CONTRACTS

FEDERALLY SPONSORED RESEARCH

Not Applicable

SEQUENCE LISTING OR PROGRAM

Not Applicable

BACKGROUND—FIELD OF INVENTION

This invention relates to computer processes that use an electronically captured, verified, and digitally stored human fingerprint as an electronic signature to digitally created and stored contracts with global access via the Internet.

BACKGROUND—DESCRIPTION OF PRIOR ART

On June 30, 2000, President Clinton signed into law the Electronic Signatures In Global and National Commerce Act (E-SIGN Act), which became effective in the United States on October 1, 2000. The E-SIGN Act implements a national uniform standard for all electronic transactions that encourages the use of electronic signatures and electronic contracts by providing legal certainty for these instruments when signatories comply with its standards. However the E-SIGN Act is also technology-neutral and does not require nor recommends a specific type or method that business and consumers must use or accept in order to create and sign their electronic contract. With regard to having a signature notarized, acknowledged, verified, or made under oath, the E-SIGN Act "removes any requirement of a stamp, seal or similar embossing device as it may apply to the performance of these functions by electronic means." The E-SIGN Act also made provisions for the legal validity of electronic records (commercial transactions, such as sales or orders), which are not in the scope of this invention.

Due to fact that the E-SIGN Act is technology-neutral, an opportunity was created for the invention of a form of electronic signature that would be both easily understood by the non-technical business and legal communities and secure from theft or fraud.

Prior to the present invention, current methods for electronic signatures were based on devices such as card keys, "smart cards", and X.509 digital certificates. These and other methods have the disadvantage of being capable of duplication or theft. Prior to this invention, no method has had the opportunity to be accepted by the legal community as a uniquely identifying an individual. For example, if a person reports that their credit card was stolen, that person is not held liable for more than a very small amount of charges made subsequent to the theft. In like manner, a contract signatory who claims that their smart card was stolen, or that their laptop computer containing their X.509 digital certificate was stolen, will not likely be held liable for any contract signatures made subsequent to the theft.

Current methods for electronic signatures also suffer from being very difficult to understand. Most contract parties are not sufficiently technically proficient to understand nor capable of distinguishing one person's "digital" signature from another. For example, consider the following computer industry definition: "To facilitate authentication, a digital signature is a cryptographic function computed as a message and a user's private key. The private key is a number or a mathematical value that is unique to the sender. The signature function produces a value unique to the private key and the fingerprint value being signed. The private key has a

mathematically related public key that anyone may use to verify the signature created by the private key." *Excerpt from U.S. Patent 6,298,445.*

Use of such a digital signature and "fingerprint value" as mentioned in the previous paragraph would require the use of a computer expert for every legal dispute involving a party's denial of signature. The expensive burden of proof for such methods, and the immense difficulty in comprehending and explaining such methods to the non-technical, hinder the acceptance of electronic contracts with electronic signatures.

A human fingerprint has long been recognized globally in court and in the public as uniquely identifying an individual. The human fingerprint is considered more reliable than a photo ID or passport as legal identification. Some commercial banks have even gone so far as to require a person's fingerprint to be stamped with ink on the back of a check for those who cash checks but do not have an account with the bank.

OBJECTS AND ADVANTAGES

This invention has the objects and advantages of:

(a) Establishing universal credibility for electronic signatures by use of a digitized version of the commonly accepted form of unique person identification: the human fingerprint.

(b) By use of an easily defensible and understandable electronic signature, provides the final piece necessary for digital contracts to become legally binding, enforceable, and defensible in court.

(c) Maintaining a signatory identification database containing all necessary personal information, the signatory's scanned fingerprint in a binary format, and the signatory's scanned fingerprint in a visually graphical image.

(d) Containing electronically stored digitally signed, verified, and sealed contracts with addendums and revisions.

(e) Providing global and instantaneous access to the construction, review, revision, and signing of digital contracts by use of an Internet Browser connected to the invention's web site and database.

(f) Enabling the electronic collaboration available to Internet users with economical communication devices, such as computer keyboard text, voice microphones, and live video cameras, for the purpose of viewing, explaining, negotiating, revising, and finalizing of contract negotiations. And,

(g) Significantly reducing the time for commercial contract completion from months to hours, since the signatories need only be present via computer, no matter where their geographical location.

SUMMARY

This invention encapsulates the long-standing, universally recognized, and easily understood, unique identification provided by a human fingerprint for purposes of providing an electronic signature for a legal contract, which unique identification is not subject to theft or fraud.

DRAWINGS – BRIEF DESCRIPTION

Three figures are provided with drawings showing the computer software component processes and representative computer hardware as used by this invention.

Fig.1 is a flow chart showing this invention's computer software component processes supporting the use of a scanned and digitized human fingerprint to be acquired, stored and available for use in providing an electronic signature.

Fig. 2 is a flow chart showing this invention's computer software component processes and repositories involved in acquiring a scanned and digitized human fingerprint for either signatory registration, or for electronically signing a contract.

Fig. 3 shows the overall process that this invention uses to create, approve, and sign electronic contracts with electronic signatures using a scanned and digitized human fingerprint.

DETAILED DESCRIPTION OF DRAWINGS, PREFERRED EMBODIMENT AND OPERATION OF INVENTION

The drawings follow a simple numbering scheme. In each figure, one through three, there is a numerical reference consisting of the figure number, a decimal point, and a figure object number. The drawings provide a visual representation of the preferred embodiment of the invention and its operation. Following is a detailed description of the preferred embodiment of the invention and its operation, which follows the specific flow of the three drawings.

FIGURE 1

Fig. 1.1 – System Administration is a set of computer software component processes that are needed to administer and maintain the electronic contract database and the electronic signature database.

Fig. 1.2 is a reference to the computer software component process for adding system users. The users are categorized as either a party to the contract or as participants to the contract negotiations. A participant is one who contributes to the contract negotiations, and so must be given access to the electronic contract, addendums, and revisions. A participant might be one that authors and revises the electronic contract, addendums and attachments, or might be one that only reviews and provides feedback during the negotiations. A participant, however, is not one who will be held liable to the terms of the contract, and so will be registered to be assigned a User ID, password, and, perhaps, digital certificate for encryption and security purposes, but will not require the scanning and digitizing of a fingerprint. A party to the contract is one who, in addition to participating in the contract negotiations, will also be held liable for the terms of the contract when signed. Consequently, a contract party must, as a signatory authority, must, in addition to the normal registration process, provide a scanned and digitized human fingerprint.

Fig. 1.3 is the decision to determine of the registrant for the electronic contract negotiations will be a participant and signatory authority, or only a participant.

Fig. 1.4 is the process for the registrant who is both a participant and a signatory authority. To support an electronic signature with this invention, the signatory authority's finger is scanned using a fingerprint scanner attached to the registrant's computer. This invention currently uses the Ethentica™ MS 3000 PC Card or USB 2500 devices for fingerprint scanning. With either device or like devices that are BioAPI (biometric application programming interface as standardized by the BioAPI Consortium) compliant products, this invention scans the registrant's fingerprint, verifies the quality of the scan, captures the minutiae points

necessary for fingerprint analysis. These minutiae points are stored as binary data in the invention's Registrant Database for later retrieval and signatory verification. A graphical representation is also constructed from the binary data, which representation will match the registrant's own fingerprint, for purposes of providing the invention's users with a visual verification of what is stored in the invention as binary data.

Fig. 1.5 is a necessary process for all registrants: participants and signatory authorities. Each registrant must be categorized as an Author, who is able to create and edit the electronic contract and its addendums and attachments; a Reviewer, who is able to view all of the electronic contract, and can provide feedback to all of the participants for that electronic contract, but who cannot make any revisions to the electronic contract; and a Signatory, who is able to electronically sign, and thereby seal, the electronic contract. A registrant can be any combination of these three roles.

FIGURE 2

Fig. 2.1 is the invention's presentation of its web pages to the electronic contract participants, through an Internet Web Browser. The invention's preferred product is the Microsoft Internet Explorer, version 5.0 or later, but is not limited to this product. The web pages present the participant with a method whereby the participant can navigate the invention's electronic contract repository and can view exact visual representations of the electronic contract and its addendums and attachments. The "Scan" button in Fig. 2.1 represents that part of this invention that is clicked by the signatory participant when necessary to scan the signatory's fingerprint for either registration or for providing an electronic signature to the electronic contract.

Fig. 2.2 is the invention's Fingerprint Module, which is computer software component that is available on the participant's computer as a Plug-In to the participant's Internet Web Browser. A Plug-In is computer software component that provides special functionality that is not ordinarily available with an Internet Web Browser. The invention's Fingerprint Module is written to work with any fingerprint scanning device that is BioAPI (biometric application programming interface as standardized by the BioAPI Consortium) compliant, such as the Ethentica™ MS 3000 PC Card or USB 2500 devices.

Fig. 2.3 shows that the invention's Fingerprint Module first determines if a human finger is detected on the scanner. The devices used by the invention are capable of accurately determining if actual and live human skin has been placed on the scanner by testing the

conductivity of the material placed on the scanner. If a live human finger has not been detected, then the invention returns to Fig. 2.2. If a live human finger is detected, then the invention proceeds to Fig. 2.4.

Fig. 2.4 shows that the invention's Fingerprint Module now determines if the fingerprint scan was of sufficient quality as to provide a verifiable and unique identification of the person's fingerprint. If not, then the invention returns to Fig. 2.2 for a re-scan. If of excellent quality, then the invention proceeds to Fig. 2.5.

Fig. 2.5 represents the inventions use of industry standard high-level encryption of the binary data captured by the fingerprint scan device. The encrypted binary data is then transmitted by the invention back to the invention's Contract/Signature Web Server. The invention's Fingerprint Module in the participant's Web Browser Plug-In is used to capture the binary data necessary for fingerprint analysis, but no fingerprint verification is performed in the participant's Web Browser or on the participant's computer. This is to be performed on the invention's remote servers, so that minimal data is transmitted over the Internet, thereby insuring security and efficiency.

Fig. 2.6 is the invention's Contract/Signature Web Server that communicates directly with the participant's Web Browser. The Web Server can consist of one or more servers, possibly clustered, as the processing demands require. The Web Server is responsible for the encryption and decryption of data with the participant's Web Browser, is responsible for basic and digital verification of the participant's identification, and is responsible for directing the participant's information requests to the appropriate invention's back-end processes as needed.

Fig. 2.7 is the invention's server process to determine if the fingerprint scan was for purposes of registration or not. If the fingerprint scan was for registration, then the invention proceeds to Fig. 2.8. If not, then the scan was performed to electronically sign an electronic contract, in which case the invention proceeds to Fig. 2.11.

Fig. 2.8 is the invention's server Fingerprint Module. This server is not necessarily the same computer as the Web server, but can be the same computer. The server Fingerprint Module analyzes the binary data sent by the Web Browser Plug-In fingerprint scan to extract the fingerprint minutiae points and other relevant information. The extract is then placed in the Registrant Database in Fig. 2.9, along with all other identifying information relevant to the registrant, who in this case is a signatory authority. If Fig. 2.9 is successful, then the invention proceeds from Fig. 2.8 to Fig. 2.10.

Fig. 2.9 is the invention's Registrant Database, which contains all identifying information pertaining to each user's identification and role in the electronic contract negotiation process. Additional information is stored that relates a registrant to the electronic contract(s) to which the registrant is a participant. This database is highly secure and can only be accessed by the invention's Server processes. No other direct access is permitted. When accessed by Server processes, the Registrant Database returns a success or fail status to Fig. 2.8.

Fig. 2.10 is the invention's process that converts the now registered fingerprint scan into a visual graphical representation that directly matches the registrant's own human fingerprint. This graphical data is returned to the registrant's Web Browser and is viewable within the invention's Web pages. This allows the registrant to visually verify that the registrant's fingerprint was successfully processed by the invention.

Fig. 2.11 is traversed by the invention from Fig. 2.7 and is the invention's Server Fingerprint Module. This is a computer process that passes the binary fingerprint scan data to the Registrant Database, along with other identifying information, for verification.

Fig. 2.12 is the invention's Registrant Database and contains the invention's server computer processes necessary for supporting the electronic signature.

Fig. 2.13 is the invention's computer process for determining if a given set of binary fingerprint scan data has a match in the set of currently registered electronic contract participants. The algorithm for matching binary fingerprint scan data is in accordance with the industry standards set by the Biometric Consortium.

Fig. 2.14 is the invention's computer process that signals whether the electronic contract participant's fingerprint is on file and is registered as a signatory authority. If the participant is not a signatory authority, then a message so indicating is returned to Fig. 2.1. If the participant is authorized to electronically sign the electronic contract, then the invention proceeds to Fig. 2.15.

Fig. 2.15 is the invention's computer process that converts the binary fingerprint scan data into a graphical representation that directly matches the registrant's own human fingerprint. This graphical data is returned to the registrant's Web Browser and is viewable within the invention's Web pages. This allows the registrant to visually verify that the registrant's fingerprint was successfully processed by the invention.

Fig. 2.16 is the invention's Contract Database that contains all electronic contracts, each contract's addendums, attachments, and all other information relevant to the electronic contract negotiations, revisions, and signing.

Fig. 2.17 is the invention's computer processes that attach the now verified binary fingerprint scan data to the electronic contract, and the electronic contract is flagged as duly signed. An updated Web page is returned to the participant's Web Browser, showing the electronically signed contract.

FIGURE 3

Fig. 3.1 references the invention's computer processes and interfaces to allow the System Administrator to administer all of the invention's databases and user information. An important process is the categorization of electronic contract participants as Author, Review, and/or Signatory. Additional human steps might need to be performed by the System Administrator or designate to verify information or provided during the registration process or to provide online assistance to the registrant.

Fig. 3.2 is the first draft of the electronic contract that results from the start of the process of the electronic negotiations conducted by the participants set up in Fig. 3.1.

Fig. 3.3 is the invention's set of computer processes that assist the electronic contract participants in revising the electronic as needed by those authorized to make such revisions. The invention provides processes that allow participants to collaborate electronically via text messages, live or recorded voice messages, and live or recorded video messages and conferencing in order to remove any geographical barriers and to significantly streamline the entire contract process. The final outcome of this process is the Final Version of the electronic contract, its addendums and attachments, which is now ready for electronic signing.

Fig. 3.4 is the invention's set of computer processes that capture each signatory authority's fingerprint, processes the data as shown in Fig. 2, and notifies each participant as to the progress of the signing.

Fig. 3.5 is the invention's set of computer processes that lock and seal electronically signed contracts to prevent any further revisions. These processes make the electronic contract and associated documents a permanent set of electronic records. Participants are electronically notified at the conclusion of the process.

While the preferred embodiment of the invention has been illustrated and described, it will be appreciated that various changes can be made therein without departing from the spirit and scope of this invention.

Conclusion, Ramifications, and Scope

Thus the reader will see that the invention provides methods and processes whereby an easily understood and defensible form of electronic signature, a digitized scan of the human fingerprint, that will allow full use of the opportunities afforded by the Electronic Signatures In Global and National Commerce Act (E-SIGN Act). Without this invention, the use of electronic contracts and electronic signatures as original documents will be mired in the failings of the prior art. This invention provides methods and processes to capture and maintain data for unique identification of persons, which data is not subject to the fraud and theft of the methods contained in prior art.

By legitimizing the entire process of electronic contract negotiations, this invention allows a significant and often critical reduction in the effort and time necessary in completing contract negotiations. The geographic boundaries between contract parties are removed by this invention's facilities to support electronic collaboration, information gathering and recording, and electronic signing. With this invention, the entire process of contract drafting, revising, finalizing, and signing remove all need of any of the parties or participants to ever be in the same room. This invention allows its users to continue with their other business and personal interests without interruption and without the costs associated with geographical meetings.

Due to its fully electronic nature in the business of contracts, use of this invention will allow a multitude of businesses to expand beyond their geographical boundaries, since all business transactions start with a contract. With this invention, the use of contracts will be limited only by the reaches of the Internet and other mediums of computer communication.

By virtue of its speed of electronic access, use of this invention will allow the sealing of business negotiations to be successful, since oftentimes any delay provides opportunity for a business deal to fail and for parties to change their mind.

Although the present invention and its advantages have been described in detail, it should be understood that various changes, substitutions and alterations can be made herein without departing from the spirit and scope of the invention as defined by the appended claims.